REMARKS/ARGUMENTS

The Office Action has been carefully considered. It is respectfully submitted that the issues raised are traversed, being hereinafter addressed with reference to the relevant headings appearing in the Detailed Action section of the Office Action.

Claim Rejections – 35 USC § 103

At page 2 of the Office Action, the Examiner has maintained rejections to claims 1, 2, 4, 6, 7, and 11 as being unpatentable over Shigenaga (US Patent No. 4,710,613) in view of Lee (US Patent No. 5,923,759).

Reconsideration and withdrawal of this rejection is respectfully requested in light of the following comments.

Although the Applicant respectfully maintains that a skilled person in the art would not be motivated to combine Shigenaga with Lee, for reasons highlighted in the Applicant's previous response, the Applicant respectfully submits that the present claim 1 is patentable over Shigenaga in view of Lee.

In particular, the combination of Shigenaga and Lee does not describe:

- applying in the trusted authentication chip a keyed one way function to a random number by using a first key, thereby producing a first encrypted outcome.
- applying in the untrusted authentication chip a keyed one way function to the random number using a second key, thereby producing a second encrypted outcome.
- comparing the first encrypted outcome and the second encrypted outcome, without knowledge of the first or second key.

The Applicant respectfully reminds that Examiner that in accordance with MPEP section 2143, in order to prove a *prima facie* case of obviousness, *the prior art reference (or references when combined)* must *teach or suggest* ***all*** *the claim limitations.* The Applicant fails to see all of the claim features in the combination of Shigenaga and Lee.

In the *Response to Arguments* section of this Office Action, the Examiner has failed to particularly point out where in the combination of Shigenaga and Lee the Examiner sees all of the claimed limitations. Consequently, it seems that the Examiner has not considered the Applicant's arguments regarding the fact that Shigenaga in view of Lee does not describe all of the claimed limitations. The Applicant respectfully reminds the Examiner that in making a final rejection, the Examiner must clearly state the reasons in support thereof (see 37 CFR 1.113(b)). Accordingly, the Applicant re-submits these arguments for consideration by the Examiner.

The Applicant maintains that claim 1 is patentable over Shigenaga in view of Lee.

On pages 5 to 6 of the Office Action, the Examiner has stated:

> *"Shigenaga does no disclose applying, in the trusted authentication chip, a key one way function to the second decrypted outcome using the second key to produce an encrypted outcome...Lee discloses the IC card performs both encrypt and decrypt function using an internal key stored in the card and the terminal card performs both encrypt and decrypt function using an identifying key stored in memory (column 6, lines 37-67)"*

However, on closer inspection of the section of Lee which the Examiner has highlighted, in fact Lee describes two **separate routines that are performed separately**.

In particular, lines 37 to 52 describes the "Authenticate Card Routine 300" which is used for *"allow[ing] system 100 to determine whether a card inserted into one of the card units is authentic"* (Column 6, lines 37 to 40). The "Authenticate Card Routine 300" comprises the steps of:

- a processor 122 generating a random number (column 6, lines 40 and 41);
- processor 122 transmits generated random number to the card (column 6, line 41);
- card receives random number; (column 6, lines 41 to 42);
- card encrypts random number using algorithm and an "internal key" (column 6, lines 42 to 43);
- card returns encrypted random number to processor 122 (column 6, line 44);

- processor 122 decrypts the encrypted number based upon same algorithm and an identifying key (column 6, lines 46 to 48); and
- processor 122 compares the original random number to the decrypted random number to determine authenticity of the card (column 6, lines 48 to 50).

In contrast to the "Authenticate Card Routine 300", as described by Lee, and outlines above, claim 1 of the present application describes:

- applying in the trusted authentication chip a keyed one way function to a random number by using a first key, thereby producing a first encrypted outcome.
- applying in the untrusted authentication chip a keyed one way function to the random number using a second key, thereby producing a second encrypted outcome.
- comparing the first encrypted outcome and the second encrypted outcome, without knowledge of the first or second key.

Thus, as shown in the comparison above, Lee does not describe having a first and a second encrypted outcome produced by the trusted and untrusted authentication chips respectfully, where the first and second encrypted outcomes are compared in order to determine whether the untrusted authentication chip is valid. In Lee, the processor in the Authenticate Card Routine 300 compares the original random number to the decrypted random number in order to determine the authenticity of the card.

Additionally, Lee does not describe the application of a first and a second key in the trusted and untrusted chips respectfully to produce the first and second encrypted outcomes. Lee only encrypts the random number once, in the processor, the random number is then returned to the card, and is decrypted. Lee does not describe separately encrypting the random numbers thereby producing two separate encrypted outcomes.

Furthermore, the Applicant highlights to the examiner that claim 1 describes comparing the first and second encrypted outcomes without knowledge of the first and second keys. In the Authenticate Card Routine 300 of Lee, the processor first decrypts the encrypted random number received based upon an algorithm and an identifying key stored in the memory 126, before comparing the original random number to the decrypted random number. Thus, the

processor has knowledge of at least one key, which is in contrast to the validation protocol of claim 1.

Thus, claim 1 of the present invention provides numerous distinctions between a combination of Shigenaga and Lee.

In a totally separate routine as shown in Figure 3, Lee describes at column 6, lines 53 to 65 the "Authenticate Host Routine 310" which is used *"to allow a card to determine whether the processing system in which the card is inserted is authentic"*. Thus, Lee describes that this routine is used by the card to determine the authenticity of the host.

Therefore "Authenticate Card Routine 300" is in total contrast to "Authenticate Host Routine 310" because "Authenticate Card Routine 300" is used for authenticating the card whereas "Authenticate Host Routine 310" is used for authenticating the host. Nowhere in Lee is it suggested that these two routines could be combined to only authenticate the card.

In any event, the routine for authenticating the host, as described by Lee, is in contrast to the present claim 1 for similar reasons as described above with respect to the card authentication routing 300.

The host authentication routine 310 does not describe having a first and a second encrypted outcome produced by the trusted and untrusted authentication chips respectfully, where the first and second encrypted outcomes are compared in order to determine whether the untrusted authentication chip is valid. In Lee, the card in the Authenticate Card Routine 310 compares the original random number to the decrypted random number in order to determine the authenticity of the processor. Furthermore, the routine 310 in Lee does not describe the application of a first and a second key in the trusted and untrusted chips respectfully to produce the first and second encrypted outcomes.

Thus, lines 37 to 67 of column 6 which the Examiner has highlighted are irrelevant to the claims. Accordingly, the combined teachings of lines 37 to 67 in column 6 of Lee and the disclosure of Shigenaga fail to teach or suggest the features of claim 1 as outlined above.

The Applicant respectfully submits that in authentication systems, these are not trivial distinctions, and claim 1 is patentable over a combination of Shigenaga and Lee.

The applicant submits that independent claims 1 and 6 are patentable over Shigenaga in view of Lee as required by MPEP at 2143.

The applicant respectfully requests that Examiner withdraw the rejection to all the claims.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 U.S.C. §103(a). The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant:

SIMON ROBERT WILAMSLEY

Applicant:

PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762